# Wykład 3

## Kwaterniony

***Definicja 1.*** *Ciałem nieprzemiennym* nazywamy zbiór $\mathbb{F}$ z działaniami dodawania $+$ i mnożenia $\cdot$ spełniającymi następujące warunki:

- oba działania są łączne;
- oba mają elementy neutralne, przy czym element neutralny dodawania jest różny od elementu neutralnego mnożenia;
- dodawanie jest przemienne;
- **mnożenie nie jest przemienne**; tzn. istnieją elementy $x$, $y$ w $\mathbb{F}$, że $x \cdot y \neq y \cdot x$;
- każdy element ciała ma element przeciwny i każdy różny od zera $-$ elementu neutralnego dodawania $-$ ma element odwrotny;
- mnożenie jest rozdzielne względem dodawania zarówno **prawo-** jak i **lewostronnie.**

***Twierdzenie 1.*** Zbiór $\mathbb{H} = \{a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k} \colon a, b, c, d \in \mathbb{R}\}$ z działaniami

- dodawania $+$

$$(x_0 + x_1\,\mathrm{i} + x_2\,\mathrm{j} + x_3\,\mathrm{k}) + (y_0 + y_1\,\mathrm{i} + y_2\,\mathrm{j} + y_3\,\mathrm{k}) = (x_0 + y_0) + (x_1 + y_1)\,\mathrm{i} + (x_2 + y_2)\,\mathrm{j} + (x_3 +$$

- mnożenia $\cdot$

$$\begin{aligned}(x_0 + x_1\,\mathrm{i} + x_2\,\mathrm{j} + x_3\,\mathrm{k}) \cdot (y_0 + y_1\,\mathrm{i} + y_2\,\mathrm{j} + y_3\,\mathrm{k}) &= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3) && (1)\\ &+ (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)\,\mathrm{i} && (2)\\ &+ (x_0y_2 - x_1y_3 + x_2y_0 + x_3y_1)\,\mathrm{j} && (3)\\ &+ (x_0y_3 + x_1y_2 - x_2y_1 + x_3y_0)\,\mathrm{k} && (4)\end{aligned}$$

jest ciałem nieprzemiennym. Jego zerem jest $0 = 0 + 0\,\mathrm{i} + 0\,\mathrm{j} + 0\,\mathrm{k}$ zaś jedynką $1 = 1 + 0\,\mathrm{i} + 0\,\mathrm{j} + 0\,\mathrm{k}$.

***Umowa.*** W wyrażeniu $a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ składniki postaci $0$, $0\,\mathrm{i}$, $0\,\mathrm{j}$, $0\,\mathrm{k}$ opuszczamy.

***Uwaga.*** Na to aby odtworzyć wzór na mnożenie wystarczy zapamiętać, że

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1 \qquad (\mathrm{ijk})$$

oraz, że liczby rzeczywiste są przemienne z symbolami $\mathrm{i}$, $\mathrm{j}$ $\mathrm{k}$; to znaczy, dla każdej rzeczywistej $x = x + 0\,\mathrm{i} + 0\,\mathrm{j} + 0\,\mathrm{k}$ mamy $x\,\mathrm{i} = \mathrm{i}\,x$, $x\,\mathrm{j} = \mathrm{j}\,x$, $x\,\mathrm{k} = \mathrm{k}\,x$.

***Zadanie 1.***

1. Wyznacz $\mathrm{jk}$ i $\mathrm{ik}$.

Strony związku $\mathrm{ijk} = -1$ mnożymy lewostronnie przez $\mathrm{i}$. Wykorzystując łączność mnożenia i przemienność mnożenia przez liczby rzeczywiste dostaniemy $\mathrm{i}^2\mathrm{jk} = -\,\mathrm{i}$. Ponieważ $\mathrm{i}^2 = -1$, więc

$$\mathrm{jk} = \mathrm{i}.$$

Teraz strony otrzymanej równości mnożymy prawostronnie przez $\mathrm{k}$: $\mathrm{jk}^2 = \mathrm{ik}$. Stąd

$$\mathrm{ik} = -\,\mathrm{j}.$$

1. Wyznacz $(2+\mathrm{i})(-\mathrm{j}+3\,\mathrm{k})$. Oznaczmy szukany element zbioru $\mathbb{H}$ przez $q$. Wtedy

$$q = -2\,\mathrm{j} + 6\,\mathrm{k} - \mathrm{ij} + 3\,\mathrm{ik}.$$

Postępując jak w punkcie 1, możemy przekonać się, że $\mathrm{ij} = \mathrm{k}$. Stąd

$$q = -5\,\mathrm{j} + 5\,\mathrm{k}.$$

Ciało nieprzemienne $\mathbb{H}$ nazywamy *ciałem kwaternionów*, a jego elementy *kwaternionami*.

Kwaterniony zostały odkryte przez Williama Rowana Hamiltona 16 października 1843. Tego dnia wyrył on wzory (ijk) w kamieniu mostu Brougham w Dublinie. Był to pierwszy znany akt wandalizmu naukowego.

Każdy kwaternion $u$, dla którego zachodzi równość $u^2 = -1$ nazywamy *jednostką urojoną*. W takim razie $\pm\mathrm{i}$, $\pm\mathrm{j}$, $\pm\mathrm{k}$ są przykładami jednostek urojonych.

Podobnie jak w przypadku ciała liczb zespolonych określamy *sprzężenie* w ciele kwaternionów:

> jeśli $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$, to $\bar{q} = a - b\,\mathrm{i} - c\,\mathrm{j} - d\,\mathrm{k}$.

Zachodzą związki:

$$q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2. \tag{qu}$$

Oczywiście

$$|q|^2 = q\bar{q} = \bar{q}q. \tag{ms}$$

Sprzężenie ma następujące własności:

$$\overline{q \pm r} = \bar{q} \pm \bar{r}, \tag{s1}$$

$$\overline{qr} = \bar{r}\bar{q}\,. \tag{s2}$$

***Komentarz.*** Wzór (s1) jest oczywisty. Wzór (s2) można sprawdzić bezpośrednio ze wzoru na iloczyn kwaternionów lub też wykorzystać wzór (s1) i fakt, że mnożenie kwaternionów z liczbami rzeczywistymi jest przemienne. Wtedy pozostaje zweryfikować prawdziwość wzoru (s2), gdy $q, r$ przybierają wartości ze zbioru $\{\mathrm{i}, \mathrm{j}, \mathrm{k}\}$.

Własności modułu:

$$|qr| = |q||r|, \tag{m1}$$

$$||q| - |r|| \le |q \pm r| \le |q| + |r| \quad (\text{nierówność trójkąta}) \tag{m2}$$

Najtrudniejszym elementem dowodu twierdzenia 1 jest wykazanie, że każdy niezerowy element ma odwrotny. Niech $q \neq 0$. Podzielmy strony związku (ms) przez liczbę rzeczywistą $|q|^2$; to znaczy, pomnóżmy przez odwrotność tej liczby. Wtedy

$$1 = q\frac{\bar{q}}{|q|^2} = \frac{\bar{q}}{|q|^2}q.$$

Stąd

$$q^{-1} = q\frac{\bar{q}}{|q|^2}.$$

### Zastosowania w teorii liczb

***Zadanie 2.*** Jeśli liczby naturalne $n$ i $m$ dają się przedstawić jako sumy dwu kwadratów liczb całkowitych, to ich iloczyn też ma takie przedstawienie. (Zadanie domowe)

***Wskazówka.*** Przeanalizować rozwiązanie zadania 3. Kwaterniony zastąpić liczbami zespolonymi.

***Zadanie 3.*** Jeśli liczby naturalne $n$ i $m$ dają się przedstawić jako sumy czterech kwadratów liczb całkowitych, to ich iloczyn też ma takie przedstawienie.

*Rozwiązanie* Niech $n = x_0^2 + x_1^2 + x_2^2 + x_3^2$, $m = y_0^2 + y_1^2 + y_2^2 + y_3^2$, gdzie wszystkie liczby $x_i$ oraz $y_i$ są całkowite. Utwórzmy kwaterniony

$$q = x_0 + x_1\,\mathrm{i} + x_2\,\mathrm{j} + x_3\,\mathrm{k}, \quad r = y_0 + y_1\,\mathrm{i} + y_2\,\mathrm{j} + y_3\,\mathrm{k}.$$

W zgodzie ze wzorem na mnożenie kwaternionów (twierdzenie 1), iloczyn $qr = z_0 + z_1\,\mathrm{i} + z_2\,\mathrm{j} + z_3\,\mathrm{k}$ ma wszystkie współczynniki $z_i$ całkowite. Ponadto, na podstawie wzorów (qu), (ms), (m1):

$$z_0^2 + z_1^2 + z_2^2 + z_3^2 = |qr|^2 = |q|^2|r|^2 = nm \qquad \square$$

***Zadanie domowe.*** Przedstawić liczbę 60 jako sumę czterech kwadratów liczb całkowitych.

## Permutacje

***Definicja 2.*** Niech $X$ oznacza niepusty zbiór o skończonej liczbie elementów. Każde odwzorowanie $\sigma\colon X \to X$ *różnowartościowe* (więc także i *na*) nazywamy permutacją zbioru $X$. Zbiór wszystkich takich permutacji oznaczamy $S_X$.

Najczęściej $X = [n] := \{1, 2, \ldots, n\}$. W takim przypadku zamiast $S_{[n]}$ piszemy $S_n$.

***Sposoby zapisywania permutacji:***

1. ***Tabelka.***

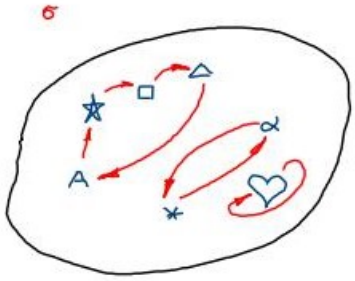
$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Np. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ oznacza taką permutację $\sigma$, że $\sigma(1) = 3$, $\sigma(2) = 1$ i $\sigma(3) = 2$.

1. ***Wiersz***. W przypadku, gdy $X = [n]$, możemy bez obawy utraty informacji górny wiersz tabelki opuścić i zapisać permutację $\sigma$ tak: $\sigma(1)\sigma(2)\ldots\sigma(n)$

Permutacja opisana w przykładzie zapisuje się tak: $312$.

1. ***Diagram strzałkowy.***



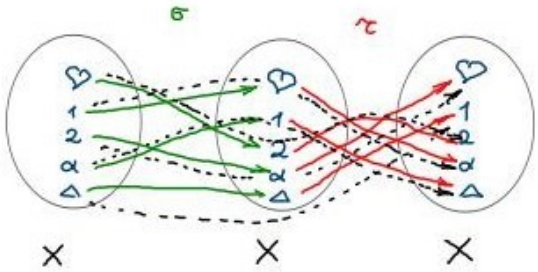

Tabelka permutacji $\sigma$ zobrazowanej na diagramie przedstawia się następująco:

$$\begin{pmatrix} A & \star & \square & \triangle & * & \alpha & \heartsuit \\ \star & \square & \triangle & A & \alpha & * & \heartsuit \end{pmatrix}$$

***Definicja 3.*** Niech $\tau, \sigma \in S_X$. *Złożeniem* $\tau\sigma$ permutacji $\sigma$ z permutacją $\tau$ określamy wzorem

$$(\tau\sigma)(x) = \tau(\sigma(x)).$$

Złożenie $\tau\sigma$ jest więc odwzorowaniem (to samo co funkcją) z $X$ w $X$.




$$\tau\sigma = \begin{pmatrix} \heartsuit & 1 & 2 & \alpha & \triangle \\ 2 & \alpha & \heartsuit & \triangle & 1 \end{pmatrix}.$$

***Lemat 2.*** Złożenie permutacji jest permutacją

*Dowód.* Niech $\tau, \sigma \in S_X$. Wystarczy wykazać różnowartościowość $\tau\sigma$. Niech $x, y \in S_X$. Przypuśćmy że $\tau\sigma(x) = \tau\sigma(y)$. Wtedy, w zgodzie z definicją złożenia,

$$\tau(\sigma(x)) = \tau(\sigma(y)).$$

Ponieważ $\tau$ jest różnowartościowa, więc $\sigma(x) = \sigma(y)$. I ponieważ także $\sigma$ jest różnowartościowa, więc $x = y$. Stąd $\tau\sigma$ jest odwzorowaniem różnowartościowym $X$ w $X$ więc permutacją.□

***Zapis.*** Złożenie $\sigma\sigma$ zapisujemy $\sigma^2$. Podobnie, $\sigma^k$ oznacza $k$-krotne złożenie permutacji $\sigma$.

***Lemat 3.*** Składanie permutacji jest łączne.

*Dowód.* Musimy wykazać, że dla wszelkich $\tau, \sigma, \rho \in S_X$

$$\tau(\sigma\rho) = (\tau\sigma)\rho.$$

Ustalmy dowolny $x \in X$. Wtedy na mocy definicji złożenia

$$\tau(\sigma\rho)(x) = \tau(\sigma(\rho(x))) = (\tau\sigma)(\rho(x)) = (\tau\sigma)\rho(x).$$

W takim razie $\tau(\sigma\rho)$ oraz $(\tau\sigma)\rho$ przyjmują na każdym argumencie $x \in X$ tę samą wartość, są więc równe. □

***Definicja 4.*** Takie odwzorowanie $\varepsilon$: $X \to X$, że dla wszelkiego $x \in X$

$$\varepsilon(x) = x$$

nazywamy *identycznościowym* albo *identycznością* na $X$.

***Spostrzeżenie.*** Identyczność na $X$ jest elementem neutralnym składania odwzorowań; to znaczy, dla wszelkiego $\tau \in S_X$

$$\varepsilon\tau = \tau\varepsilon = \tau.$$

***Lemat 4.*** Dla wszelkiego $\sigma \in S_X$ istnieje $\tau \in S_X$, że

$$\tau\sigma = \sigma\tau = \varepsilon.$$

*Dowód.* Ustalmy $y \in X$. Ponieważ $\sigma$ jest odzorowaniem *na*, więc istnieje $x \in X$, że $\sigma(x) = y$. Co więcej taki $x$ jest jedyny, bo odzwzorowanie $\sigma$ jest różnowartościowe. Wystarczy teraz przyjąć $\tau(y) = x$. $\square$.

***Komentarz.*** Permutacja $\tau$ zapewniona przez Lemat 4 jest po prostu elementem odwrotnym do $\sigma$ względem działania składania. Oznaczamy ją zwykle $\sigma^{-1}$. Jeśli $\sigma$ jest dana tabelką, to tabelka permutacji odwrotnej powstaje przez przestawienie wierszy. Np. permuatcja $\sigma$, zadana wcześniej diagramem strzałkowym, ma jako odwrotną permutację

$$\sigma^{-1} = \begin{pmatrix} \star & \square & \triangle & A & \alpha & * & \heartsuit \\ A & \star & \square & \triangle & * & \alpha & \heartsuit \end{pmatrix}$$

Co trzeba zmienić w diagramie strzałkowym, aby otrzymać diagram permutacji odwrotnej?

***Definicja 5.*** Zbiór $G$ z działaniem $\bullet$ nazywamy *grupą* jeśli działanie to jest łączne, ma element neutralny $e$ oraz każdy element $g \in G$ ma element odwrotny. Jeśli działanie jest przemienne, to grupę nazywamy *przemienną* albo *abelową*. W przeciwnym razie jest ona *nieprzemienna*.

Lematy 2−4 prowadzą do następującego twierdzenia:

***Twierdzenie 5.*** Niech $X$ niepusty zbiór o skończonej liczbie elementów. Zbiór $S_X$ ze składaniem jako działaniem jest grupą.

***Uwaga.*** Zestawię teraz przykłady grup rozpatrywanych na poprzednich wykładach.

1. Jeśli wziąć dowolne ciało $\mathbb{F}$, to $\mathbb{F}$ z działaniem dodawania tworzy grupę przemienną.
2. Niech $\mathbb{F}^*$ oznacza zbiór wszystkich niezerowych elementów ciała bądź ciała nieprzemiennego $\mathbb{F}$. Zbiór ten z działaniem mnożenia tworzy grupę. W przypadku ciał nieprzemiennych jest to grupa nieprzemienna.
3. Dla każdej liczby naturalnej $n > 1$, $\mathbb{Z}_n$ jest z dodawaniem $\oplus$ grupą przemienną. Jest to tak zwana grupa cykliczna rzędu $n$. Odgrywa ona podstawową rolę w rozmaitych zastosowaniach.
4. Zbiory $\mathbb{S} = \{z \in \mathbb{C}\colon |z| = 1\}$ oraz $\mathbb{S}^3 = \{q \in \mathbb{H}\colon |q| = 1\}$ są grupami z działaniami mnożenia liczb zespolonych w pierwszym przypadku i kwaternionów w drugim.

Symbolem $\binom{X}{2}$ oznaczmy zbiór wszystkich par nieuporządkowanych $\{x, y\}$, że $x, y \in X$ oraz $x \neq y$.

Niech $\sigma \in S_n$ i niech $x, y \in [n]$ będą różne. Mamy

$$\frac{\sigma(x)-\sigma(y)}{x-y}=\frac{\sigma(y)-\sigma(x)}{y-x}.$$

W rezultacie wielkość $\frac{\sigma(x)-\sigma(y)}{x-y}$ zależy jedynie od pary nieuporządkowanej $\{x,y\}$. Uwaga ta objaśnia poprawność następującej definicji:

***Definicja 6.***

Dla permutacji $\sigma\in S_n$, $n>1$, określamy jej *znak* $\operatorname{sgn}(\sigma)$ w następujący sposób:

$$\operatorname{sgn}(\sigma)=\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\sigma(x)-\sigma(y)}{x-y}$$

***Spostrzeżenie.*** Jeśli $\varepsilon\in S_n$ jest permutacją identycznościową, to

$$\operatorname{sgn}(\varepsilon)=1.$$

***Lemat 6.*** Dla każdej pary permutacji $\sigma,\tau\in S_n$

$$\operatorname{sgn}(\sigma)=\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\sigma(\tau(x))-\sigma(\tau(y))}{\tau(x)-\tau(y)}.$$

*Dowód.* Niech $x'=\tau(x)$, $y'=\tau(y)$. Można łatwo się przekonać, że odwzorowanie $\{x,y\}\mapsto\{x',y'\}$ jest permutacją zbioru $\binom{[n]}{2}$. Stąd

$$\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\sigma(\tau(x))-\sigma(\tau(y))}{\tau(x)-\tau(y)}=\prod_{\{x',y'\}\in\binom{[n]}{2}}\frac{\sigma(x')-\sigma(y')}{x'-y'}=\operatorname{sgn}(\sigma).$$

02.11.20 Tutaj skończyłem.

***Twierdzenie 7.*** Niech $n>1$. Dla wszelkich $\sigma,\tau\in S_n$

1. $\operatorname{sgn}(\sigma\tau)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$,
2. $\operatorname{sgn}(\sigma)\in\{-1,1\}$.

*Dowód.*

$$\begin{aligned}\operatorname{sgn}(\sigma\tau)&=\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\sigma(\tau(x))-\sigma(\tau(y))}{x-y}=\prod_{\{x,y\}\in\binom{[n]}{2}}\left(\frac{\sigma(\tau(x))-\sigma(\tau(y))}{\tau(x)-\tau(y)}\cdot\frac{\tau(x)-\tau(y)}{x-y}\right)\\&=\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\sigma(\tau(x))-\sigma(\tau(y))}{\tau(x)-\tau(y)}\prod_{\{x,y\}\in\binom{[n]}{2}}\frac{\tau(x)-\tau(y)}{x-y}\\&=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\end{aligned}$$

Przy czym ostatnia z równości jest konsekwencją lematu 6.

Przejdźmy do dowodu drugiej części twierdzenia.

Niech $A=\{|\operatorname{sgn}(\kappa)|\colon\kappa\in S_n\}$ i niech $m=\min A$ oraz $M=\max A$. Wystarczy wykazać, że $m=M=1$. W tym celu wybierzmy takie permutacje $\rho$ i $\sigma\in S_n$, że $m=|\operatorname{sgn}(\rho)|$ oraz $M=|\operatorname{sgn}(\sigma)|$. Na podstawie części pierwszej i definicji $m,M$

$$m \leq |\operatorname{sgn}(\rho^2)| = \operatorname{sgn}(\rho)^2 = m^2.$$

I podobnie,

$$M \geq |\operatorname{sgn}(\sigma^2)| = \operatorname{sgn}(\sigma)^2 = M^2.$$

Stąd $1 \leq m \leq M \leq 1$. Co oczywiście pociąga $m = M = 1$.□

***Ważne spostrzeżenie.*** Z definicji znaku permutacji i twierdzenia 7 wynika, że $\operatorname{sgn}(\sigma) = (-1)^s$, gdzie

$$s = \text{liczba tych par } \{x, y\}, \text{ że } \frac{\sigma(x) - \sigma(y)}{x - y} < 0.$$

Inaczej,

$$s = \text{liczba tych par } \{x, y\}, \text{ że } \sigma \text{ odwraca ich porządek.}$$

***Przykład.*** Rozpatrzmy permutacje $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ oraz $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$. Zbiór par, których porządek $\sigma$ odwraca, to $\{\{1,3\},\{1,5\},\{2,3\},\{2,5\},\{4,5\}\}$. Stąd $\operatorname{sgn}(\sigma) = (-1)^5 = -1$. Zbiór par, których porządek $\tau$ odwraca, to $\{\{1,2\},\{1,4\},\{1,5\},\{2,4\},\{2,5\},\{3,4\},\{3,5\}\}$. Stąd $\operatorname{sgn}(\tau) = (-1)^7 = -1$. Na podstawie twierdzenia 7, $\operatorname{sgn}(\sigma\tau) = 1$.

Możemy też obliczyć znak $\sigma\tau$ wprost z definicji: $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$. Zbiór par, których porządek $\sigma\tau$ odwraca, to $\{\{1,2\},\{1,3\},\{1,4\},\{1,5\}\}$. Stąd powtórnie $\operatorname{sgn}(\sigma\tau) = (-1)^4 = 1$.

***Zadanie 4.*** (Wszystkie rozpatrywane permutacje należą do $S_n$, $n > 1$). Wykazać, że

1. Permutacje $\sigma$ i $\sigma^{-1}$ mają ten sam znak.
2. Jeśli $\tau$ jest permutacją nieparzystą, to $\tau^3\sigma\tau^2\sigma^{-3}$ jest także permutacja nieparzystą.

***Wniosek 8.*** Niech $\sigma_1, \sigma_2, \ldots, \sigma_s \in S_n$ − dowolny skończony ciąg permutacji. Wtedy

$$\operatorname{sgn}(\sigma_1\sigma_2\cdots\sigma_s) = \prod_{i=1}^{s} \operatorname{sgn}(\sigma_i).$$

Niech $A_n$ oznacza podzbiór grupy $S_n$ złożony ze wszystkich permutacji *parzystych*, to znaczy takich, które mają znak $1$. Zbiór ten z działaniem składania permutacji jest grupą. Jest ona znana jako *grupa alternująca* zbioru $[n]$. Dodajmy, że permutacje o znaku $-1$ nazywamy *nieparzystymi*.

## Cykle

***Definicja 7.*** Przypuśćmy, że $x_1, x_2, \ldots, x_k$ to ciąg różnych i niekoniecznie wszystkich elementów zbioru $X$. Permutację $\sigma \in S_X$ określoną w ten sposób, że

- $\sigma(x_i) = x_{i+1}$, dla $i = 1, \ldots, k-1$,
- $\sigma(x_k) = x_1$
- $\sigma(x) = x$, dla $x \in X \setminus \{x_1, \ldots, x_k\}$

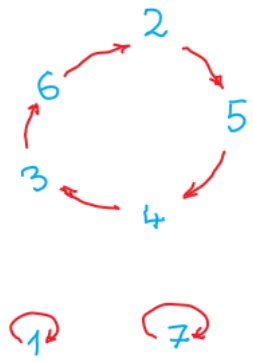
nazywamy *cyklem długości* $k$. Cykl ten często zapisujemy tak: $\sigma = (x_1 x_2 \ldots x_k)$ względnie tak $\sigma = (x_1, x_2, \ldots, x_k)$. Cykle długości dwa nazywamy *transpozycjami* lub *przestawieniami*.

***Uwaga.*** Napisy $(x_1x_2\dots x_k)$, $(x_2x_3\dots x_kx_1)$ itd. oznaczają ten sam cykl.

***Przykład.*** Permutacja

$$\kappa = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 6 & 3 & 4 & 2 & 7 \end{pmatrix}$$

jest cyklem długości $5$. Możemy go zapisać tak: $\kappa = (2\,5\,4\,3\,6)$. Proszę zauważyć, że $1$ i $7$, które są *punktami stałymi* permutacji $\kappa$ – to znaczy, $\kappa(1) = 1$ i $\kappa(7) = 7$ – zostały pominięte. Permutację $\kappa$ możemy przedstawić na diagramie strzałkowym:

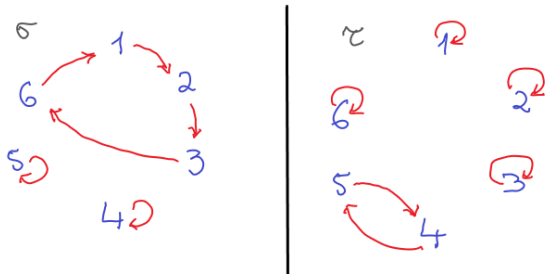



Elementy cyklu $(2\,5\,4\,3\,6)$ zostały rozłożone kołowo. (Cykl, od greckiego κύκλος, to tyle co koło.)

***Definicja 8.*** Dwie permutacje $\sigma$ i $\tau$ zbioru $X$ nazywamy *rozłącznymi* jeśli dla wszelkiego $x \in X$:

$$\sigma(x) \neq x \Rightarrow \tau(x) = x \quad \text{oraz} \quad \tau(x) \neq x \Rightarrow \sigma(x) = x$$

Permutacje na poniższej ilustracji są rozłączne.




Akurat przedstawione permutacje są cyklami. Ogólnie, dwa cykle $(x_1x_2\dots x_k)$ oraz $(y_1y_2\dots y_l)$ są rozłączne wtedy i tylko wtedy, gdy ciągi $x_1, x_2, \dots, x_k$ oraz $y_1, y_2, \dots, y_l$ nie mają wspólnych wyrazów.

***Stwierdzenie 9*** Jeśli dwie permutacje $\sigma$ i $\tau \in S_X$ są rozłączne, to są także przemienne.

*Dowód.* Należy wykazać, że dla wszelkiego $x \in X$

$$\tau(\sigma(x)) = \sigma(\tau(x)). \qquad (\text{ab})$$

Jeśli $\sigma(x) \neq x$, to wobec różnowartościowości $\sigma$ także $\sigma(\sigma(x)) \neq \sigma(x)$. Wtedy, wobec definicji rozłączności, mamy $\tau(\sigma(x)) = \sigma(x)$ oraz $\tau(x) = x$, co pociąga $\sigma(\tau(x)) = \sigma(x)$. Łącząc oba skrajne związki dostaniemy (ab).

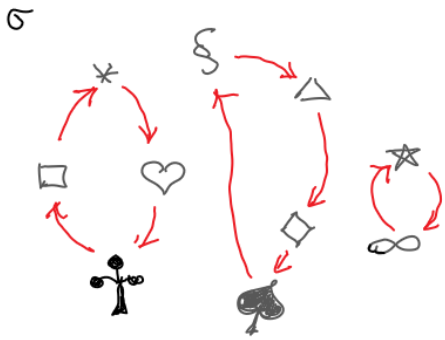
W taki sam sposób dowodzimy, że jeśli $\tau(x) \neq x$, to równość (ab) także zachodzi Do rozpatrzenia pozostaje przypadek $\sigma(x) = x = \tau(x)$. Wtedy jednak

$$\tau(\sigma(x)) = x = \sigma(\tau(x)).$$

□

***Stwierdzenie 10.*** Każdą permutację można przedstawić w postaci złożenia parami rozłącznych cykli.

Nietrudny dowód pominiemy. Zamiast niego zrobimy kilka ilustracji. Rozkład permutacji na cykle rozłączne możemy łatwo wywnioskować z diagramu strzałkowego:



Mianowicie $\sigma = (* \heartsuit \clubsuit \square)(\S \triangle \diamondsuit \spadesuit)(\star \infty)$

Jeśli permutacja jest zapisana w postaci tabelki, to rozkład na cykle także jest łatwo odczytać. Niech np.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 8 & 7 & 2 & 5 & 1 \end{pmatrix}.$$

Bierzemy pierwszy wyraz górnego wiersza: $1$, dopisujemy odpowiadającą mu wartość: $3$, dopisujemy wartość odpowiadającą $3$: $4$, dopisujemy wartość odpowiadajacą $4$: $8$. Wartością odpowiadającą $8$ jest $1$. Cykl się zamknął. Jest nim $(1\,3\,4\,8)$. Bierzemy skrajny lewy wyraz w górnym wierszu niezawarty w cyklu: $2$. Odpowiada mu wartość $6$, a tej wartości znowu odpowiada $2$. Mamy następny cykl $(2\,6)$. Wybieramy skrajny lewy wyraz górnego wiersza, którego nie ma w wypisanych już cyklach: $5$. Jemu odpowiada wartość $7$, a tej znowu $5$. Otrzymaliśmy ostatni cykl $(5\,7)$. Stąd $\sigma = (1\,3\,4\,8)(2\,6)(5\,7)$. Ponieważ cykle są rozłączne, więc w świetle stwierdzenia 8 ich kolejność w rozkładzie nie odgrywa roli.

**Znak cyklu**

Rozpocznijmy od wyznaczenia znaku cyklu $(1\,2\,3\ldots k) \in S_n$, $2 \leq k \leq n$. Sporządźmy tabelkę tego cyklu:

$$\begin{pmatrix} 1 & 2 & \ldots & k-1 & k & k+1 & \ldots & n \\ 2 & 3 & \ldots & k & 1 & k+1 & \ldots & n \end{pmatrix}$$

Zbiór par, których porządek cykl odwraca przedstawia się następująco:
$\{(1,k),(2,k),\ldots,(k-1,k)\}$. Jest ich $k-1$. Stąd

$$\operatorname{sgn}(1\,2\,3\ldots k) = (-1)^{k-1} \qquad (\mathrm{cp})$$

Wykażemy, że powyższy wzór ma miejsce dla dowolnego cyklu długości $k$ w $S_n$.

***Stwierdzenie 11.*** Dla każdego cyklu $\sigma$ długości $k \leq n$ w $S_n$ zachodzi wzór

$$\operatorname{sgn}(\sigma) = (-1)^{k-1}$$

*Dowód.* Niech $\sigma = (x_1 x_2 \ldots x_k)$. Wybierzmy taką permutację $\tau \in S_n$, że $\tau(i) = x_i$ for $i = 1,\ldots,k$. Wtedy

$$\tau^{-1}\sigma\tau = (1\,2\,3\ldots k) \qquad (\mathrm{aut})$$

Z twierdzenia 7,

$$\begin{aligned}\operatorname{sgn}(\tau^{-1}\sigma\tau) &= \operatorname{sgn}(\tau^{-1})\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau^{-1})\operatorname{sgn}(\tau) && (8)\\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau^{-1}\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\varepsilon) && (9)\\ &= \operatorname{sgn}(\sigma) && (10)\end{aligned}$$

Stąd i ze wzorów (cp) i (aut) otrzymujemy tezę. □

*Wniosek 12.* Jeśli $\sigma \in S_n$ jest złożeniem cykli $\sigma_s, \ldots, \sigma_2, \sigma_1$ o długościach $k_s, \ldots, k_2, k_1$, to

$$\operatorname{sgn}(\sigma) = (-1)^{k_1+k_2+\cdots+k_s-s}$$

***Uwagi.***

1. Cykle dlatego napisano wspak, by $\sigma = \sigma_1\sigma_2\cdots\sigma_s$.
2. Wniosek 12 może zostać użyty do efektywnego obliczania znaków permutacji. Wystarczy permutację rozłożyć na cykl, tzn. przedstawić jako złożenie cykli.
3. Wniosek 12 podpowiada także jak określić znak permutacji należącej do $S_X$, gdzie $X$ dowolny zbiór skończony. Wystarczy rozłożyć ją na cykle i przyjąć, że wniosek zachodzi także w tym ogólnym przypadku. Np. niech $\sigma$ będzie permutacją omówioną przy okazji diagramów strzałkowych. Jej rozkład na cykle przedstawia się następująco:

   $$\sigma = (A \star \square\triangle)(*\alpha).$$

   Stąd $\operatorname{sgn}(\sigma) = (-1)^{4+2-2} = 1$.

**Rozkład permutacji na transpozycje**

Każdy cykl $(x_1x_2\ldots x_k)$, $k > 2$ możemy przedstawić w postaci złożenia transpozycji:

$$(x_1x_2\ldots x_k) = (x_1x_k)(x_1x_{k-1})\cdots(x_1x_2).$$

W takim razie każdą permutację $\sigma$ zbioru liczącego przynajmniej dwa elementy możemy zapisać w postaci złożenia pewnej liczby transpozycji:

$$\sigma = \tau_1\tau_2\cdots\tau_t.$$

złożenie takie nazywamy także rozkładem permutacji na transpozycje. W zgodzie z wnioskiem 12, $\operatorname{sgn}(\sigma) = (-1)^t$. Otrzymaliśmy kolejny

*Wniosek 13.* Dla każdej pary rozkładów permutacji na transpozycje liczba czynników w rozkładzie ma tę sama parzystość.